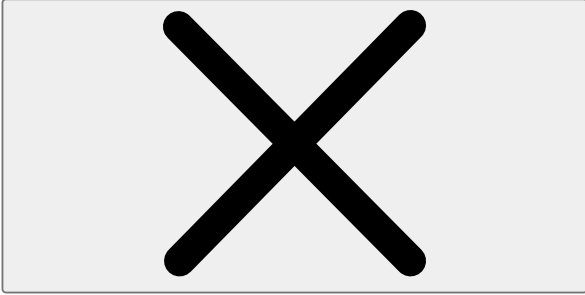


x



Search

Unstoppable Innovations CrowdCast Series: From Red-Hot Releases to Future Roadmap Register now

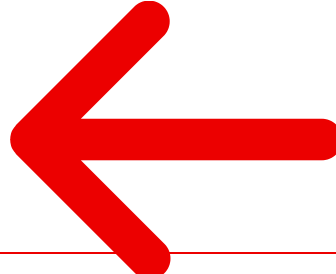
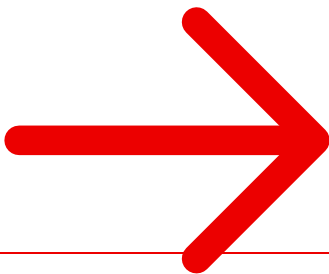


[Skip to Main Content](#)

- [Experienced a Breach?](#)
- [Small Business](#)
- [+ CrowdStrike Marketplace](#)
- [📞 Contact Us](#)
- [📡 Blog](#)



- [Platform](#)



[Explore](#)

[Platform](#)

# The Definitive AI-Native Cybersecurity Platform

- [Endpoint Detection & Response](#) The leader in endpoint security backed by pioneering adversary intelligence and native AI.
- [Exposure Management](#) The leader in exposure management with complete attack surface visibility and AI-powered vulnerability management.
- [Identity Threat Detection & Response](#) Stop modern attacks in real time with the only unified platform for identity protection and endpoint security.
- [IT Automation](#) Consolidate security and IT with one platform, agent, and console to cut complexity and cost.
- [Threat Intelligence & Hunting](#) The leader in cyber threat intelligence with world-class research and elite threat hunting to disrupt adversaries.
- [Cloud Security](#) The most complete CNAPP with unified agent and agentless protection, from code to cloud.
- [Next-Gen SIEM](#)  
The world's only AI-native SOC platform that consolidates siloed security tools and data.
- [Generative AI](#) Turn hours of work into minutes or seconds with generative AI workflows for cybersecurity and IT.
- [Data Protection](#)  
Unified data protection that deploys instantly on existing agents to stop the theft of sensitive information.
- [Workflow Automation](#) Build your own workflows with native security orchestration, automation, and response (SOAR).

- [Services](#)  
[Prepare](#)

---

[Prepare and train your organization to defend against sophisticated threat actors using real-life simulation exercises.](#)

[SEC Readiness Services](#)

[Tabletop Exercise](#)

[Red Team/Blue Team Exercise](#)

[Adversary Emulation Exercise](#)

[Penetration Testing](#)

[Respond](#)

---

[Available under a Services Retainer, giving you access to security consultants and expertise to respond to a breach.](#)

[Incident Response](#)

[Compromise Assessment](#)

[Endpoint Recovery](#)

[Network Detection](#)

[Experienced a breach?](#)

[Fortify](#)

---

[Enhance your cybersecurity practices and controls with actionable recommendations to fortify your cybersecurity posture.](#)

[Maturity Assessment](#)

[Technical Risk Assessment](#)

[SOC Assessment](#)

[Cloud Security Assessment](#)

[Identity Security Assessment](#)

[Managed Services](#)

---

[Managed Detection & Response](#)

[Included in Falcon Complete and backed by CrowdStrike's Breach Prevention Warranty.](#)

[Cloud Detection and Response](#)

[The only CDR that unifies world-class threat intelligence and 24/7 services with the world's most complete CNAPP.](#)

[Additional Services](#)

---

[Cloud Security Services](#)

[Identity Protection Services](#)

[Falcon LogScale Services](#)

[Partner Services](#)

- [Why CrowdStrike](#)  
[Why CrowdStrike](#)

---

[Considering Microsoft?](#)

[Cyber risk that starts with Microsoft ends with CrowdStrike](#)

[Read more](#)

[Compare CrowdStrike](#)

[See how we stack up against our competitors](#)

[Industry Recognition](#)

[CrowdStrike is the recognized leader in endpoint protection solutions.](#)

[MITRE ATT&CK](#)

[CrowdStrike achieves industry-leading coverage for MITRE AT&CK evaluations.](#)

[Customer Stories](#)

[Don't take our word for it, hear what our customers have to say.](#)

[Solutions by Topic](#)

---

[Cloud Detection and Response](#)

[The only CDR that unifies world-class threat intelligence and 24/7 services with the world's most complete CNAPP.](#)

[Zero Trust](#)

[Real-time breach protection on any endpoint, cloud workload or identity, wherever they are.](#)

[Ransomware Protection](#)

[Learn what you can do to stop ransomware threats in their tracks.](#)

[Observability & Log Management](#)

[Fills in the gaps, logs everything, and realizes real-time observability for your entire system.](#)

[Log4Shell Mitigation](#)

[Get the latest information on this evolving vulnerability.](#)

[Solutions by Industry](#)

---

[Small Business](#)

[Election Security](#)

[State and Local Government](#)

[Federal Government](#)

[Healthcare](#)

[Education](#)

[Financial Services](#)

[Retail](#)

- [Learn](#)

[Featured Resources](#)

---

[Considering Microsoft?](#)

[Cyber risk that starts with Microsoft ends with CrowdStrike](#)

[Cybersecurity 101 Glossary](#)

[Explanations, examples and best practices on a variety of cybersecurity topics.](#)

[Get Your Threat Landscape](#)

[Discover the adversaries targeting your industry.](#)

[2024 Global Threat Report](#)

[The must-read cybersecurity report of the year.](#)

[2023 Threat Hunting Report](#)

[CrowdStrike's threat hunting insights from July 1, 2022 to June 30, 2023.](#)

[CrowdStrike Blog](#)

---

[Under The Wing](#)

[Discover how CrowdStrike protects you against the most advanced attacks.](#)

[From The Front Lines](#)

[Executive Viewpoint](#)

[Counter Adversary Operations](#)

[Customer Focused](#)

---

[Free Trial Guide](#)

[Customer Support Portal](#)

[CrowdStrike University](#)  
[CrowdStrike Tech Center](#)  
[Developer Portal](#)  
[Knowledge Resources](#)

---

[Case Studies](#)  
[White Papers](#)  
[Webinars](#)  
[Adversary Universe Podcast](#)  
[Reports](#)  
[Logging Guides](#)  
[Try interactive demos](#)  
[All Resources](#)  
• [Company](#)  
[Connect With Us](#)

---

[Careers](#)  
[Events](#)  
[Fal.Con 2024](#)  
[Falcon Encounter Hands-on Labs](#)  
[Partner Programs](#)

---


[Channel Partners and Distributors](#)  
[Service Providers](#)  
[Strategic Technology Partners](#)  
[CrowdStrike Marketplace](#)  
[View All](#)  
[Become a partner](#)  
[About Us](#)

---


[Our Story](#)  
[Board of Directors](#)  
[Investor Relations](#)  
[CrowdStrike & F1 Racing](#)  
[Executive Team](#)  
[Latest News](#)  
[Environment, Social & Governance](#)



•  [Login](#)

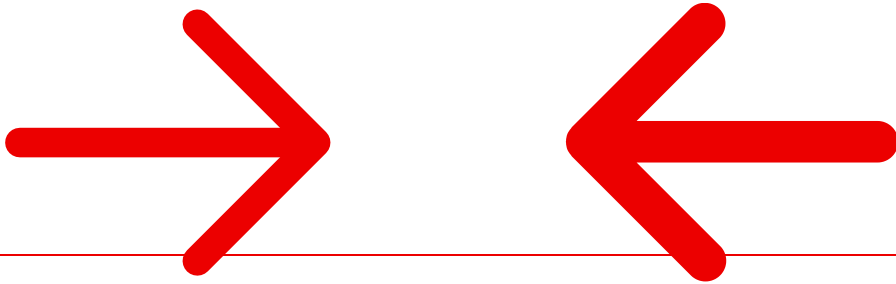


English



- - [Deutsch](#)
  - [English \(AU\)](#)
  - [English \(UK\)](#)
  - [English \(US\)](#)
  - [Español](#)
  - [Français](#)
  - [Italiano](#)
  - [LatAm](#)
  - [Português](#)
  - [عربي](#)

- - [日本語](#)
  - [繁體中文](#)
  - [한국어](#)



[View bundles &](#)

[pricing.](#)



- [View bundles & pricing](#)
- Platform
- Services
- Why CrowdStrike
- Learn
- Company
- [Blog](#)
- [Marketplace](#)
- [Login](#)
- [Contact us](#)
- [Experienced a breach?](#)
- Languages

Back

Cybersecurity 101 › Cloud Security › 12 Cloud Security Issues:  
Risks, Threats, and Challenges

# 12 CLOUD SECURITY ISSUES: RISKS, THREATS, AND CHALLENGES

[Request CNAPP Demo](#)

David Puzas - April 1, 2024

All companies face security risks, threats, and challenges every day. Many think these terms all mean the same thing, but they're more nuanced. Understanding the subtle differences between them will help you better protect your cloud assets.

What is the difference between risks, threats, and challenges?

- A **risk** is a potential for loss of data or a weak spot.
- A **threat** is a type of attack or adversary.
- A **challenge** is an organization's hurdles in implementing practical cloud security.

Let's consider an example: An API endpoint hosted in the cloud and exposed to the public Internet is a **risk**, the attacker who tries to access sensitive data using that API is the **threat** (along with any specific techniques they could try), and your organization's **challenge** is effectively protecting public APIs while keeping them available for legitimate users or customers who need them.

**A complete cloud security strategy addresses all three aspects**, so no cracks exist within the foundation. You can think of each as a different lens or angle with which to view cloud security. A solid strategy must mitigate risk (security controls), defend against threats (secure coding and deployment), and overcome challenges (implement cultural and technical solutions) for your business to use [the cloud](#) to grow securely.



## 2023 CLOUD RISK REPORT

Find out which top cloud security threats to watch for in 2023 and learn how best to address them to stay protected through 2024.

[Download Now](#)



# 4 Cloud Security Risks

You cannot completely eliminate risk; you can only manage it. Knowing common risks ahead of time will prepare you to deal with them within your environment. **What are four cloud security risks?**

1. [Unmanaged Attack Surface](#)
2. [Human Error](#)
3. [Misconfiguration](#)
4. [Data Breach](#)

## 1. Unmanaged Attack Surface

An [attack surface](#) is your environment's total exposure. The adoption of [microservices](#) can lead to an explosion of publicly available workload. Every workload adds to the attack surface. Without close management, you could expose your infrastructure in ways you don't know until an attack occurs.

No one wants that late-night call.

Attack surface can also include subtle information leaks that lead to an attack. For example,

CrowdStrike's team of threat hunters found an attacker using sampled DNS request data gathered over public WiFi to work out the names of S3 buckets. CrowdStrike stopped the attack before the attackers did any damage, but it's a great illustration of risk's ubiquitous nature. Even strong controls on the S3 buckets weren't enough to completely hide their existence. As long as you use the public Internet or cloud, you're automatically exposing an attack surface to the world.

Your business may need it to operate, but keep an eye on it.

## **2. Human Error**

According to Gartner, through 2025, 99% of all cloud security failures will be due to some level of human error. Human error is a constant risk when building business applications. However, hosting resources on the public cloud magnifies the risk.

The cloud's ease of use means that users could be using APIs you're not aware of without proper controls and opening up holes in your perimeter.

Manage human error by building strong controls to help people make the right decisions.

One final rule — don't blame people for errors. Blame the process. Build processes and guardrails to help people do the right thing. Pointing fingers doesn't help your business become more secure.

### **3. Misconfiguration**

Cloud settings keep growing as providers add more services over time. Many companies are using more than one provider.

Providers have different default configurations, with each service having its distinct implementations and nuances. Until organizations become proficient at securing their various cloud services, adversaries will continue to exploit [misconfigurations](#).

### **4. Data breaches**

A [data breach](#) occurs when sensitive information leaves your possession without your knowledge or permission. Data is worth more to attackers than anything else, making it the goal of most attacks.

Cloud misconfiguration and lack of runtime protection can leave it wide open for thieves to steal.

The impact of data breaches depends on the type of data stolen. Thieves sell personally identifiable information (PII) and personal health information (PHI) on the dark web to those who want to steal identities or use the information in phishing emails.

Other sensitive information, such as internal documents or emails, could be used to damage a company's reputation or sabotage its stock price. No matter the reason for stealing the data, breaches continue to be an imposing threat to companies using the cloud.

## **How to manage cloud security risks**

Follow these tips to manage risk in the cloud:

- Perform regular risk assessments to find new risks.
- Prioritize and implement security controls to mitigate the risks you've identified (CrowdStrike can help).

- Document and revisit any risks you choose to accept.

## LEARN MORE

Identify cloud security misconfigurations and deviations from cloud security best practices with CrowdStrike's cloud security assessment services.

**Cloud Security Assessment >**

## 4 cloud security threats

A threat is an attack against your cloud assets that tries to exploit a risk. **What are four common threats faced by cloud security?**

1. [Zero-Day Exploits](#)
2. [Advanced Persistent Threats](#)  
[Insider Threats](#)

## 3. Cyberattacks

### 1. Zero-day exploits

Cloud is “someone else’s computer.” But as long as you’re using computers and software, even those run in another organization’s data center, you’ll encounter the threat of zero-day exploits.

Zero-day exploits target vulnerabilities in popular software and operating systems that the vendor hasn’t patched. They’re dangerous because even if your cloud configuration is top-notch, an attacker can exploit zero-day vulnerabilities to gain a foothold within the environment.

### 2. Advanced persistent threats

An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged time.

APTs aren’t a quick “drive-by” attack. The attacker stays within the environment, moving from workload to workload, searching for sensitive information to

steal and sell to the highest bidder. These attacks are dangerous because they may start using a zero-day exploit and then go undetected for months.

### **3. Insider threats**

An [insider threat](#) is a cybersecurity threat that comes from within the organization — usually by a current or former employee or other person who has direct access to the company network, sensitive data and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

### **4. Cyberattacks**

A [cyber attack](#) is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Common cyberattacks performed on companies include [malware](#), [phishing](#), [DoS](#) and [DDoS](#), [SQL Injections](#), and [IoT](#) based attacks.

# How to handle cloud security threats

There are so many specific attacks; it's a challenge to protect against them all. But here are three guidelines to use when protecting your cloud assets from these threats and others.

- Follow secure coding standards when building microservices
- Double and triple check your cloud configuration to plug any holes
- With a secure foundation, go on the offensive with threat hunting. (CrowdStrike can help)

## EXPERT TIP

Protect your cloud environment from security threats with the industry's most complete cloud native application protection platform (CNAPP) with unified visibility across your cloud and apps.



## **4 cloud security challenges**

Challenges are the gap between theory and practice. It's great to know you need a [cloud security strategy](#). But where do you start? How do you tackle cultural change? What are the daily practical steps to make it happen?

**What are four cloud security challenges every company faces when embracing the cloud?**

- 1.** [Lack of Cloud Security and Skills](#)
- 2.** [Identity and Access Management](#)
- 3.** [Shadow IT](#)
- 4.** [Cloud Compliance](#)

### **1. Lack of cloud security strategy and skills**

Traditional data center security models are not suitable for the cloud. Administrators must learn new

strategies and skills specific to cloud computing.

Cloud may give organizations agility, but it can also open up vulnerabilities for organizations that lack the internal knowledge and skills to understand security challenges in the cloud effectively. Poor planning can manifest itself in misunderstanding the implications of the shared responsibility model, which lays out the security duties of the cloud provider and the user. This misunderstanding could lead to the exploitation of unintentional security holes.

## **2. Identity and access management**

[Identity and Access Management \(IAM\)](#) is essential. While this may seem obvious, the challenge lies in the details.

It's a daunting task to create the necessary roles and permissions for an enterprise of thousands of employees. There are three steps to a holistic IAM strategy: role design, privileged access management, and implementation.

Begin with a solid role design based on the needs of those using the cloud. Design the roles outside of any specific IAM system. These roles describe the work your employees do, which won't change between cloud providers.

Next, a strategy for privileged access management (PAM) outlines which roles require more protection due to their privileges. Tightly control who has access to privileged credentials and rotate them regularly.

Finally, it's time to implement the designed roles within the cloud provider's IAM service. This step will be much easier after developing these ahead of time.

### **3. Shadow IT**

[Shadow IT](#) challenges security because it circumvents the standard IT approval and management process.

Shadow IT is the result of employees adopting cloud services to do their jobs. The ease with which cloud resources can be spun up and down makes controlling its growth difficult. For example,

developers can quickly spawn workloads using their accounts. Unfortunately, assets created in this way may not be adequately secured and accessible via default passwords and misconfigurations.

The adoption of DevOps complicates matters. Cloud and DevOps teams like to run fast and without friction. However, obtaining the visibility and management levels that the security teams require is difficult without hampering DevOps activities.

DevOps needs a frictionless way to deploy secure applications and directly integrate with their [continuous integration/continuous delivery \(CI/CD\) pipeline](#). There needs to be a unified approach for security teams to get the information they need without slowing down DevOps. IT and security need to find solutions that will work for the cloud — at DevOps' velocity.

## **4. Cloud compliance**

Organizations have to adhere to regulations that protect sensitive data like [PCI DSS](#) and [HIPAA](#).

Sensitive data includes credit card information, healthcare patient records, etc. To [ensure compliance](#)

standards are met, many organizations limit access and what users can do when granted access. If access control measures are not set in place, it becomes a challenge to monitor access to the network.

## **EXPERT TIP**

Stay up to date with the most common cloud security frameworks meant to protect your environments and all sensitive data that lives within.

**Cloud Security Frameworks >**

## **How to overcome cloud security challenges**

Each challenge is different and therefore requires unique solutions. Take the time to plan before making use of any cloud services. A sound strategy takes

into consideration any common cloud challenges like the ones we've discussed here. Then you'll have a plan of action for each anticipated challenge.

## Experienced a cloud breach?

Contact the CrowdStrike's Services team to quickly establish visibility of attacker activity, work with your team

to contain the breach, and get your organization back to business faster.

[Contact Us](#)



## GET TO KNOW THE AUTHOR

David Puzas is a proven cybersecurity, cloud and IT services marketer and business leader with over two decades of experience. Charged with building client value and innovative outcomes for companies such as CrowdStrike, Dell SecureWorks and IBM clients world-wide. He focuses on the optimization of computing innovation, trends, and their business implications for market expansion and growth. David is

responsible for strategically bringing to market CrowdStrike's global cloud security portfolio as well as driving customer retention.

## Featured Articles



## What is Cyber Espionage?

# Cloud Security Architecture

 **CROWDSTRIKE**  
CYBERSECURITY 101

**Cloud Security Architecture**



A dark, abstract graphic with geometric shapes and a circular element resembling a target or a camera lens. The text "CROWDSTRIKE CYBERSECURITY 101" is prominently displayed in the center.

# CROWDSTRIKE CYBERSECURITY 101

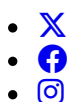
## Managed Cloud Security.

Start your  
free trial now.

Total protection has never been easier. Take advantage of our free 15-day trial and explore the most popular solutions for your business:

- Protect against malware with next-gen antivirus.
- Get unrivaled visibility with USB device control.
- Simplify your host firewall management.
- Defeat adversaries with automated threat intelligence.

[Request free trial](#)



- [in](#)
- [▶](#)

New to CrowdStrike?

[About the platform](#)

[Explore products](#)

[Services](#)

[Why choose CrowdStrike?](#)

Company

[About CrowdStrike](#)

[Careers](#)

[Events](#)

[Newsroom](#)

[Partners](#)

[CrowdStrike Marketplace](#)

Learn with CrowdStrike

[2024 Global Threat Report](#)

[Cybersecurity 101](#)

[Your Threat Landscape](#)

[Tech Center](#)

[View all resources](#)

[Contact us](#)

[Experienced a breach?](#)

Copyright © 2024

- [Contact us](#)
- [Privacy](#)
- [Cookies](#)
- [Your Privacy Choices](#)
- [Terms of Use](#)
- [Accessibility](#)